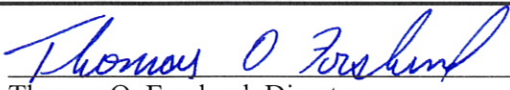


Thomas O. Forslund, Director

Governor Matthew H. Mead

Policy Title:	Electronic Device and Media Controls
Policy Number:	S-014
Effective Date:	July 1, 2013
Approval:	<div style="display: flex; justify-content: space-between;"><div> Thomas O. Forslund, Director</div><div><u>5/21/13</u> Date</div></div>

Purpose:

Wyoming Department of Health (WDH) is committed to maintaining formal practices to monitor the receipt, removal, and movement of electronic devices into, out of, and within WDH work locations. This policy ensures the control of all electronic devices and media that contain confidential or sensitive information, including protected health information (PHI).

Scope:

This policy applies to all WDH workforce.

Definition(s):

Electronic media means electronic storage media, including memory devices, and any removable/transportable digital memory medium used to exchange information already in electronic storage media.

Policy:**1. General**

- a. WDH shall establish and maintain electronic device and media control program(s) as a security standard.
- b. The electronic device and media control program(s) shall consist of the following:
 - i. Accountability;
 - ii. Receipt;
 - iii. Electronic media reuse;
 - iv. Disposal;
 - v. Data backup and storage; and
 - vi. Mobile device.

2. Accountability

- a. All electronic media that arrives at WDH shall remain in the protective packaging until inventoried and a chain of custody is established. If the electronic media will store PHI, only individuals authorized to access PHI shall access the electronic media.
- b. When electronic media that contains confidential or sensitive information is created, received, or moved within or outside of WDH, its movement and the name of the workforce member responsible for the movement shall be documented. Documentation shall include:
 - i. Workforce member's name;
 - ii. Description of the information;
 - iii. Reason for the movement; and
 - iv. Date and time.

- c. If electronic media containing PHI is to be transferred to an off-site location, all data on the electronic media shall be encrypted, and the encryption and decryption keys shall be protected with the same care as the data.
 - d. Electronic media tracking mechanisms shall be implemented to track the accountability of electronic media into and out of WDH.
 - e. A business associate agreement shall be implemented before an electronic device or media containing confidential or sensitive information is released for off-site maintenance or storage.
- 3. Receipt.** WDH shall develop an asset inventory management process to record, at a workforce member level, the movement of hardware and electronic media into and out of WDH. Asset inventories shall include:
- a. Data contained on removable, re-usable magnetic electronic data storage media, such as tapes, diskettes or CD-ROMS.
 - b. Data contained on the hard drives of file servers, disk storage arrays, mainframe, minimum or mid-range computers or diagnostic equipment.
 - c. Data contained on hard drives or personal computers that are transferred within the organization to another user, as well as those that are removed from WDH, recycled, or otherwise discarded.
 - d. Data contained on electronic computing devices, including lap or desk computers and any other related electronic devices.
 - e. Backup electronic media, including what information is stored on the backup electronic media device and the location of storage, including both on-site and off-site storage locations.
- 4. Electronic Media Reuse**
- a. Electronic media that contains electronic protected health information (ePHI) shall not be reused without proper destruction of the data. Proper destruction of data includes degaussing, physical destruction, or overwriting the entire electronic media at least once with pseudorandom data.
 - b. Following destruction, the electronic media shall be tested to ensure destruction is complete prior to the device transfer.
 - c. The method of destruction, record of new user assignment, and date, time, and signature of the person tasked with destruction shall be logged in the asset inventory list.
- 5. Disposal**
- a. When no longer needed, all electronic devices and media containing ePHI shall be physically destroyed, degaussed, or overwritten at least once with pseudorandom data.
 - b. If a third party contractor is utilized for disposal, the electronic devices or media shall be marked as containing ePHI before they go off-site, and a business associate agreement shall be in place.
 - c. The method of destruction, and date, time, and signature of the person who conducted the process shall be logged.
- 6. Backup Data and Storage**
- a. All ePHI shall be backed up on a daily basis to some form of electronic media and stored in an appropriate setting.
 - b. Electronic media containing ePHI shall be stored in a physically separate, environmentally appropriate location from where the backup resides.
 - c. Backup of all ePHI shall be created using a secure format.
 - d. Restoration procedures shall be tested at least weekly.

Contacts:

De Anna Greene, CIPP/US, CIPP/G, CIPP/IT, WDH Privacy/Compliance Officer, (307) 777-8664
Tate Nuckols, JD, WDH Security Officer, (307) 777-2438

Forms:

Building Number-Location Request Form and Instructions
Electronic Item Disposal Instructions
Fixed Asset Disposal-PP4C
IT Inventory-Update Process
WDH-63 Fixed Asset-Inventory Form
What Should I Update on My Inventory List?

Policies:

S-022; Mobile Devices
S-010; Physical Security

References:

45 CFR § 164.310(d)(1)
45 CFR § 160.103

Training: